



BLOCKCHAIN COMMONS

**GORDIAN ENVELOPE, ELISION, AND
CONTROLLER DOCUMENTS**

Welcome to Blockchain Commons



Blockchain Commons

Creating Open & Interoperable,
Secure & Compassionate Digital
Infrastructure

 [GitHub](#)

 [Discussions](#)

 [Twitter](#)

MAIN SITE

[Home](#)

[Vision](#)

[Projects](#)

[Posts](#)

[About](#)

Thank you to [the HRF](#) for a Bitcoin Development grant for our [continued support of FROST](#). We will be holding [FROST events](#) on September 18 & December 4 for library implementers, cryptographers, and wallet developers. Sign up to [our announcements lists](#) to be sure you're notified. (6/5/24)

Advocating for the creation of open, interoperable, secure & compassionate digital infrastructure to enable people to control their own digital destiny and to maintain their human dignity online


Blockchain Commons works with developer communities to design, build, and maintain secure & compassionate decentralized architectures & tools for digital assets & digital identity based on responsible key management; based on our [Gordian Principles](#) of independence, privacy, resilience, and openness; and based on our [Self-Sovereign Identity Principles](#). Our goal is to reclaim human dignity & authority in the digital world. We also strive to educate & grow the blockchain community through online courses and our work with legislators and regulators.

Blockchain Commons is proudly a "not-for-profit" social benefit corporation, domiciled in Wyoming but operating world-wide. We have a strong commitment to open source and a defensive patent strategy: anyone can use or improve our tools, and no one can take them away.


Read more about Blockchain Commons' [vision & objectives](#).



GORDIAN




Blockchain Commons

RESEARCH 

#SmartCustody

The Use of Advanced Cryptographic Tools to Improve the Care, Maintenance, Control, and Protection of Digital Assets

Christopher Allen & Shannon Appelcline



WOLF MCNALLY
BLOCKCHAIN COMMONS



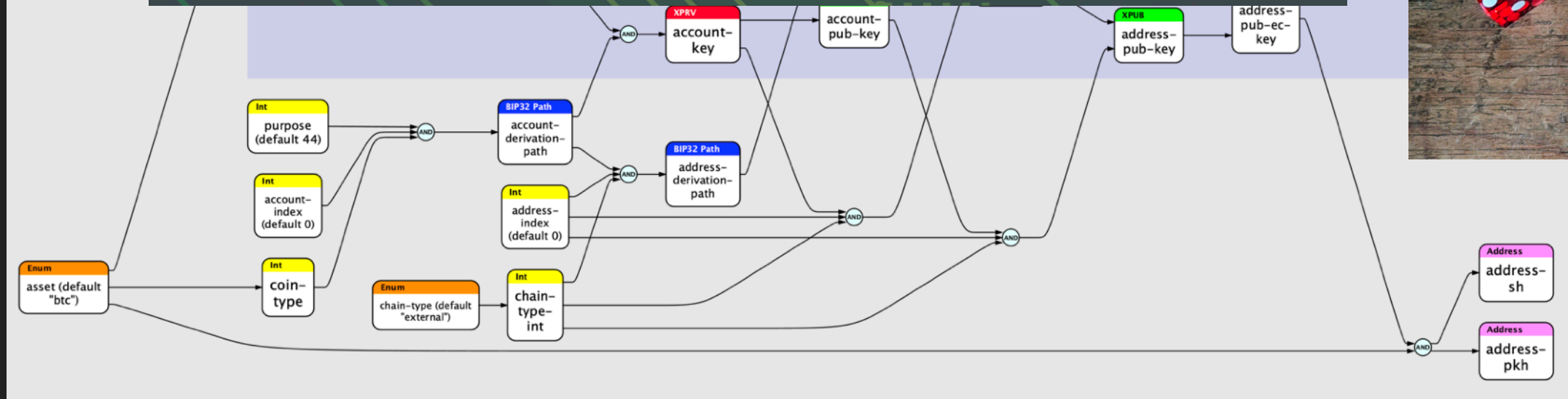
LIFEHASH

SILICON SALON



Crypto Commons

Gordian Reference Code & CLI Utilities



```
100000,
00000msat",
594d23ca15efe379e5f4a7
...
ected": true,
te": "CHANNELD_AWAITING_LOCKIN",
annel_sat": 100000,
r_amount_msat": "100000000msat",
annel_total_sat": 100000,
mount_msat": "100000000msat",
funding_txid": "f768c6e97eb2916b154976a7d8f305c76c601b3c02afd5687d5f
funding_output": 1
```

 **LEARNING BITCOIN**
FROM THE COMMAND LINE



Sustaining Sponsors

Thank you to the following companies who have become [sustaining sponsors](#).



Sustaining Sponsors



GitHub Sponsorship



BTCPay Donations



Blockchain Commons Main Site Developers Advocacy Smart Custody Sponsors

Join the Blockchain Commons Conversation

To continue the discussions of our interoperable work, Blockchain Commons hosts:

1. Discussions forums on Github.
2. Low-volume announcement lists.
3. Signal groups.

Please join us for topics that interest you!

Gordian Developers

Blockchain Commons holds a monthly Gordian Developer Meeting, usually on the first Wednesday of the month, typically at the Europe-friendly time of 10am PT. This meeting is for wallet developers and engineers working on specs for wallet developers to exchange their newest advances and to ask their newest questions. *Please join us!*

If you'd like to become a member of the Gordian Developer community, and receive announcements about upcoming meetings and the release of new resources, you can do so by joining us on Signal, participating in our Discussions forums, or subscribing to our low-volume Gordian Developers announcement list.

You can find our Signal group at:

BlockchainCommons / Gordian

Welcome to the Gordian User Community

General Discussion · shannona

is:open

Sort by: Latest activity Label Filter: Open New discussion

Categories

- View all discussions
- Bug Reports
- Feature Requests
- General Discussion
- Polls
- Questions & Answers

Most helpful Last 30 days

- wolfmcnally 1

Discussions

- Want to use bc-envelope-rust but unsure about seed/key management danpape asked 4 days ago in Questions & Answers · Answered 5
- Ask Your Questions shannona asked on Jun 15, 2021 in Questions & Answers · Unanswered 6
- Welcome to the Gordian User Community shannona started on Jun 15, 2021 in General Discussion 0
- File Your Feature Requests! shannona started on Jun 15, 2021 in Feature Requests 55
- File Your Bug Reports! shannona started on Jun 15, 2021 in Bug Reports 0
- Use SnapKit for Wallet app arhuguyenbitmark started on Oct 26, 2020 in General Discussion 4
- Gordian Server GUI after restart "frozen" henkvancann started on Oct 24, 2020 in Feature Requests 5
- Welcome to Gordian Wallet & Server Discussions! ChristopherA started on Sep 16, 2020 in General Discussion 4

Gordian Developer Community Thu, Sep 26

Christopher Allen

Blockchain Commons

Advocating for the Creation of Open, Interoperable, Secure, and Compassionate Digital Infrastructure

FROST Round Table II (2024): Overview

Docs & information on Blockchain Commons specifications. developer.blockchaincommons.com

We have posted details (video, presentations, key quotes, URLs to projects and papers, etc.) for last FROST Implementers meeting at developer.blockchaincommons.com/meeting2/

Christopher Allen (@ChristopherA) The second FROST Implementers meeting will have many of the challenges they're facing. https://t.co/YQv11BGsjx.com https://x.com/ChristopherA/status/1544444444

Christopher Allen If you're implementing (or planning) meeting will have many of the FROST challenges they're facing. If you'd like to make a pre-meeting meeting, let us know!

Ken Sedgwick Interesting new feature from the r... > Write your ncryptsec to an NFC tag, insert your password activist and if your phone is configured with a public key. Ncryptsec is a NIP-49 and dispose the NFC tag. https://github.com/vitorpamplona/amethyst/releases



- ▶ Discussion Forums
- ▶ Low-volume announcements
- ▶ Signal Groups
- ▶ Monthly Gordian Developer meetings (1st Wednesday)
- ▶ Special Meetings (FROST implementers, Silicon Salon, and more!)



Join the Conversation



RECAP

OUR INTRO MATERIALS



- ▶ Videos

- ▶ Envelope playlist on [youtube.com/@blockchaincommons](https://www.youtube.com/@blockchaincommons)
- ▶ Gordian Envelope Teaser
- ▶ Understanding Gordian Envelope, Parts 1 and 2



- ▶ Web sites

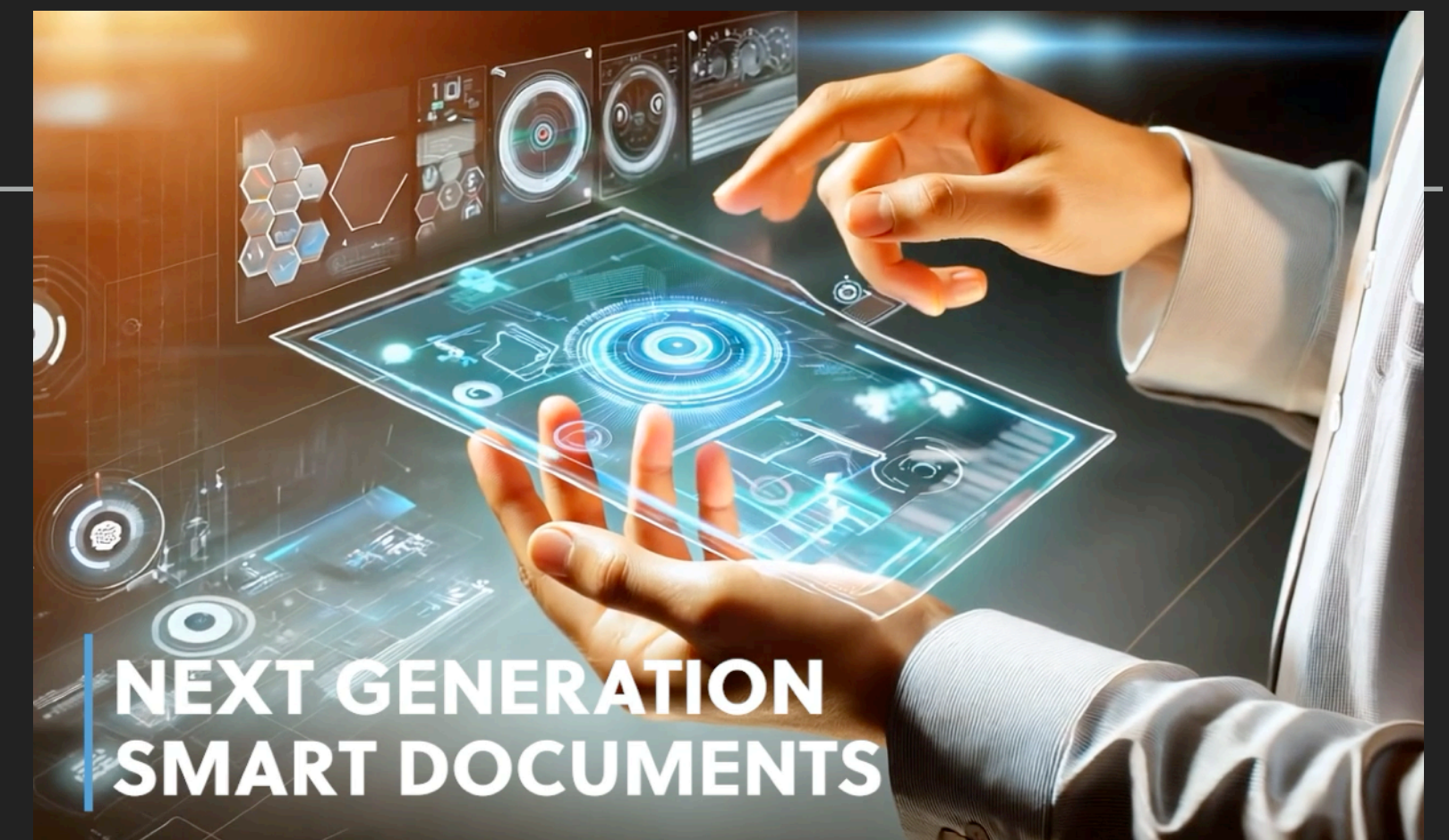
- ▶ <https://developer.blockchaincommons.com/envelope/>



DCBOR



- ▶ Envelope is a smart document system
- ▶ Built on **deterministic CBOR (dCBOR)**
 - ▶ Binary, Concise, Self-Describing, Good for IOT and constrained environments, Platform/Language agnostic
- ▶ Deterministic at the binary level up
 - ▶ One way to encode each numeric value (no 0, -0.0, 0.000, etc.)
 - ▶ Strings always Unicode Normalization Form C (NFC)
 - ▶ Map (dictionary) keys automatically sorted
 - ▶ No context required to sort
 - ▶ Never a need to canonicalize as a separate step!

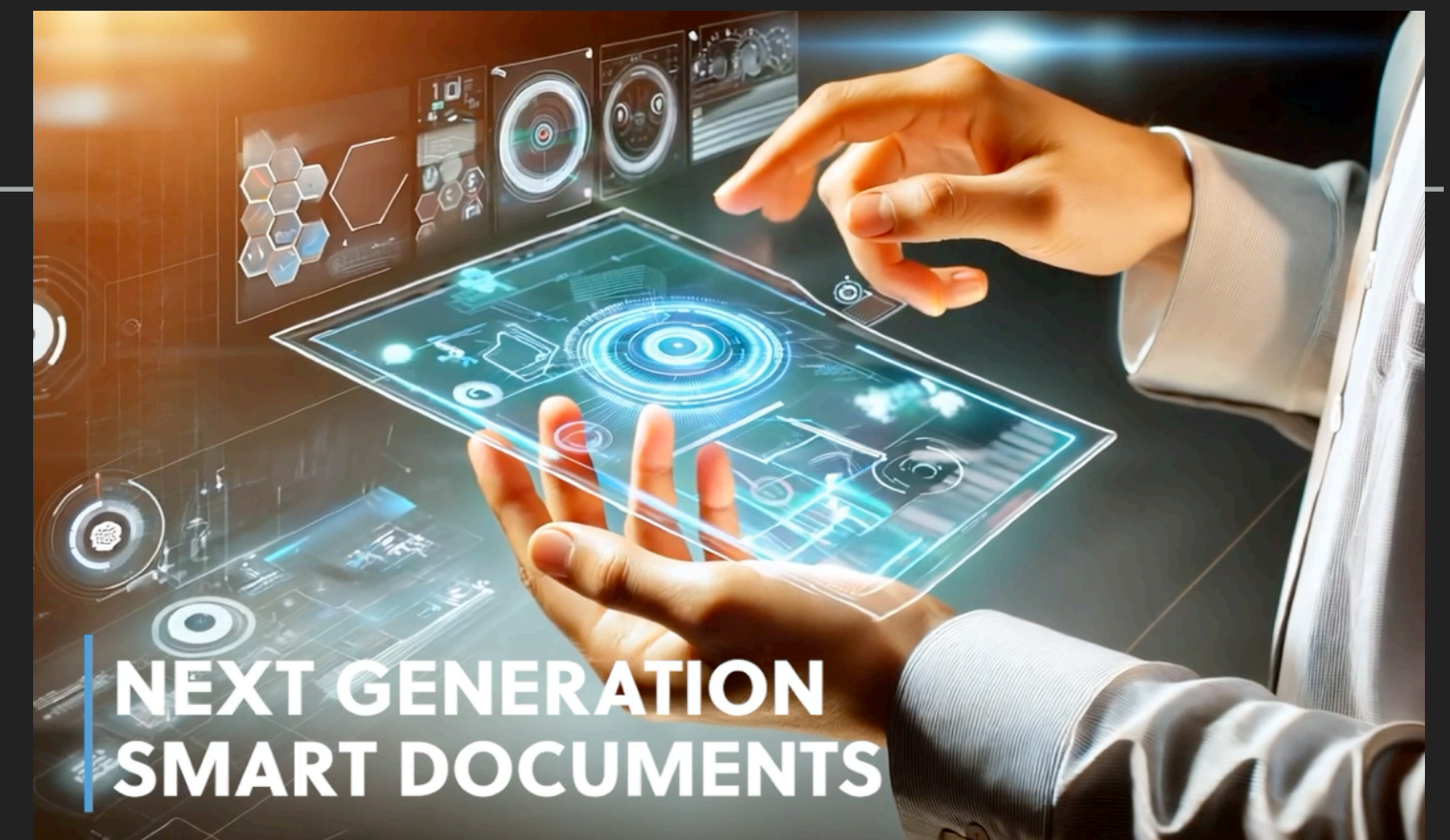


GORDIAN ENVELOPE SEMANTIC STRUCTURE

- ▶ Defines semantic triples
- ▶ subject-predicate-object

```
<subject> [  
    <predicate>: <object>  
    <predicate>: <object>  
    ...  
]
```

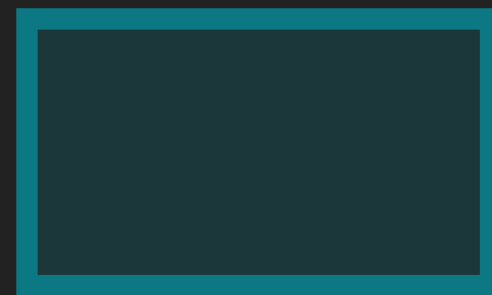
- ▶ **Note:** this is not typically the meaning of "subject" used in the Verifiable Credentials domain: "a person or organization about which claims are made."
- ▶ But in some cases it *can* be.



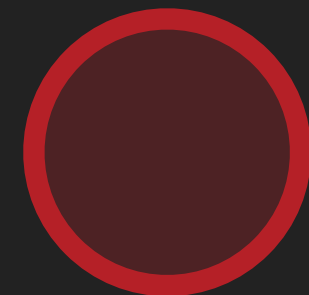
GORDIAN ENVELOPE CASES



► Five basic cases



LEAF



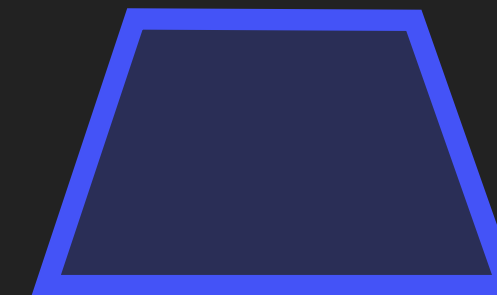
NODE



ASSERTION



ELIDED



WRAPPED

► Three extension cases



ENCRYPTED



KNOWN VALUE



COMPRESSED

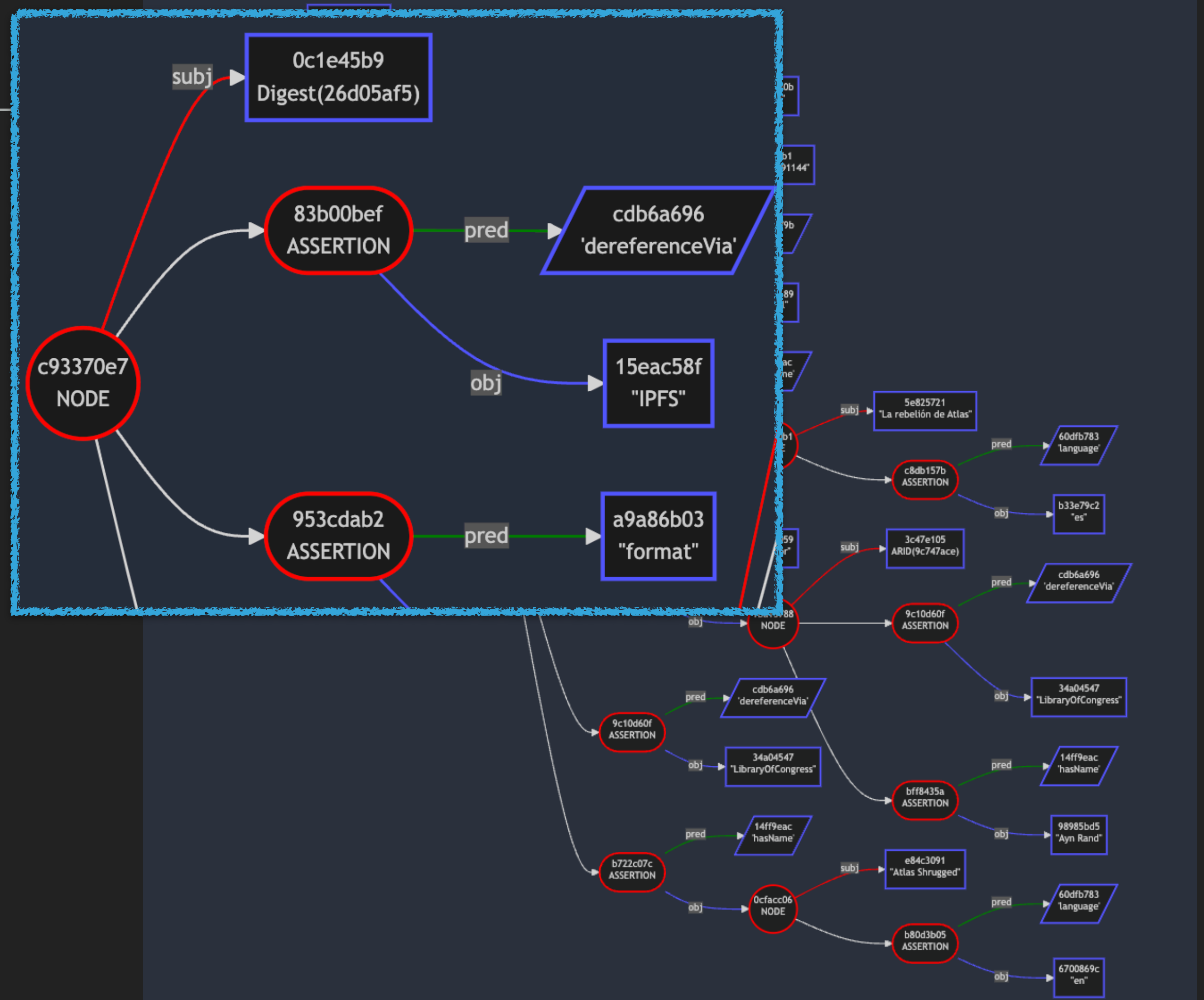


IT'S ENVELOPES ALL THE WAY DOWN!



IT'S ENVELOPES ALL THE WAY DOWN!

- ▶ Every node in envelope's tree *is* an envelope!
- ▶ NODE and ASSERTION cases have child nodes.
- ▶ Any child node without assertions can be replaced by a NODE with assertions. This includes predicates!
- ▶ Even a complete ASSERTION can become the subject of a NODE
- ▶ Every node in the tree has a unique digest.
- ▶ Certain transformations preserve the top-level digest:



- ▶ Elision
- ▶ Encryption
- ▶ Compression



ELIDED



ENCRYPTED



COMPRESSED



ELISION: THE GAME-CHANGER

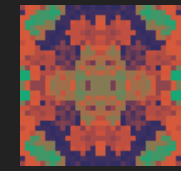


ELIDED

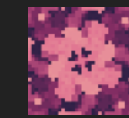


- ▶ Only transmit the data you want!
- ▶ Signatures are preserved as long as the digest tree maintains proof of the elided data
- ▶ Inclusion proofs allow you to reveal parts of the document later in a verifiable way.

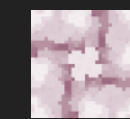




}



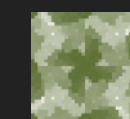
"E281029" [



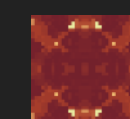
'isA': "Driver License"



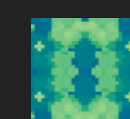
"firstName": "John"



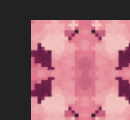
"lastName": "Doe"



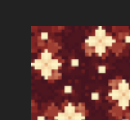
"photograph": 😊



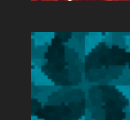
"dateOfBirth": 1994-07-30



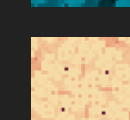
"address": "123 Elm St., Town USA"



"issuer": "State of Example"



"issued": 2021-03-17



"expires": 2029-03-17

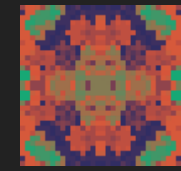
]

} [

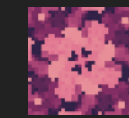
'verifiedBy': Signature

]





}



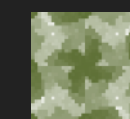
"E281029" [



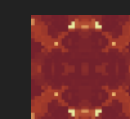
'isA': "Driver License"



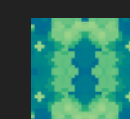
"firstName": "John"



"lastName": "Doe"



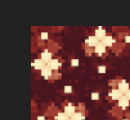
"photograph": 😊



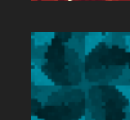
"dateOfBirth": 1994-07-30



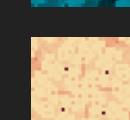
"address": "123 Elm St., Town USA"



"issuer": "State of Example"



"issued": 2021-03-17



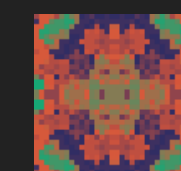
"expires": 2029-03-17

]

}

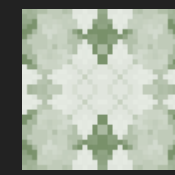
[

'verifiedBy': Signature

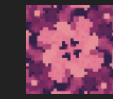


]





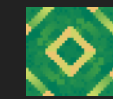
}



"E281029" [



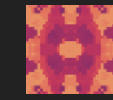
'isA': "Driver License"



"firstName": "John" [

'salt': Salt

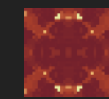
]



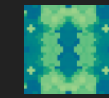
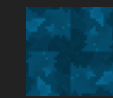
"lastName": "Doe" [

'salt': Salt

]



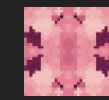
"photograph": 😊



"dateOfBirth": 1994-07-30 [

'salt': Salt

]



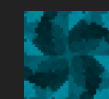
"address": "123 Elm St., Town USA" [

'salt': Salt

]



"issuer": "State of Example"



"issued": 2021-03-17



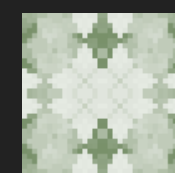
"expires": 2029-03-17

]

}

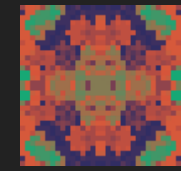
[

'verifiedBy': Signature



]





}

```
"E281029" [  
  'isA': "Driver License"  
  "firstName": "John"  
  "lastName": "Doe"  
  "photograph": 😊  
  "dateOfBirth": 1994-07-30  
  "address": "123 Elm St., Town USA"  
  "issuer": "State of Example"  
  "issued": 2021-03-17  
  "expires": 2029-03-17  
]
```

}

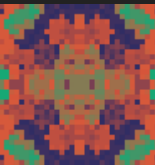
[

```
'verifiedBy': Signature
```

]





```
{  
  "E281029" [  
    'isA': "Driver License"  
    "firstName": "John"  
    "lastName": "Doe"  
    "photograph": 😊  
    "dateOfBirth": 1994-07-30  
    "address": "123 Elm St., Town USA"  
    "issuer": "State of Example"  
    "issued": 2021-03-17  
    "expires": 2029-03-17  
  ]  
} [  
  'verifiedBy': Signature   
]
```



“Prove your date of birth from your photo.”





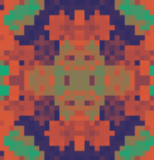
```
    {  
      ELIDED [  
        'isA': "Driver License"  
        "photograph": 😊  
        "dateOfBirth": 1994-07-30  
        "issuer": "State of Example"  
        ELIDED (5)  
      ]  
    } [  
      'verifiedBy': Signature   
    ]
```



“Prove your date of birth from your photo.”



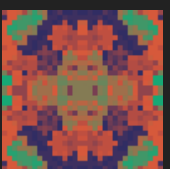


```
{  
  ELIDED [  
    'isA': "Driver License"  
    "photograph": 😊  
    "dateOfBirth": 1994-07-30  
    "issuer": "State of Example"  
    ELIDED (5)  
  ]  
  [  
    'verifiedBy': Signature   
  ]  
}
```

“Now prove where you live.”





```
{  
  ELIDED [  
    'isA': "Driver License"  
    "photograph": 😊  
    "dateOfBirth": 1994-07-30  
    "issuer": "State of Example"  
    "address": "123 Elm St., Town USA"  
    ELIDED (4)  
  ]  
} [  
  'verifiedBy': Signature   
]
```



“Now prove where you live.”





❖ "address": "123 Elm St., Town USA"

Inclusion Proof



EXTENSIONS: GORDIAN SEALED TRANSACTION PROTOCOL (GSTP)



EXTENSIONS: GORDIAN SEALED TRANSACTION PROTOCOL (GSTP)

- ▶ Establish key agreement
- ▶ Exchange data
- ▶ Facilitate confidential backups
- ▶ Coordinate multisig sessions
- ▶ ...securely and without local state!



EXTENSIONS: GORDIAN SEALED TRANSACTION PROTOCOL (GSTP)



```
{
  request(ARID(c66be27d)) [
    'body': «do_it» [
      <arg1>: Type1
      <arg2>: Type2
    ]
    'senderPublicKey': PublicKeyBase
  ]
} [
  'verifiedBy': Signature
]
```



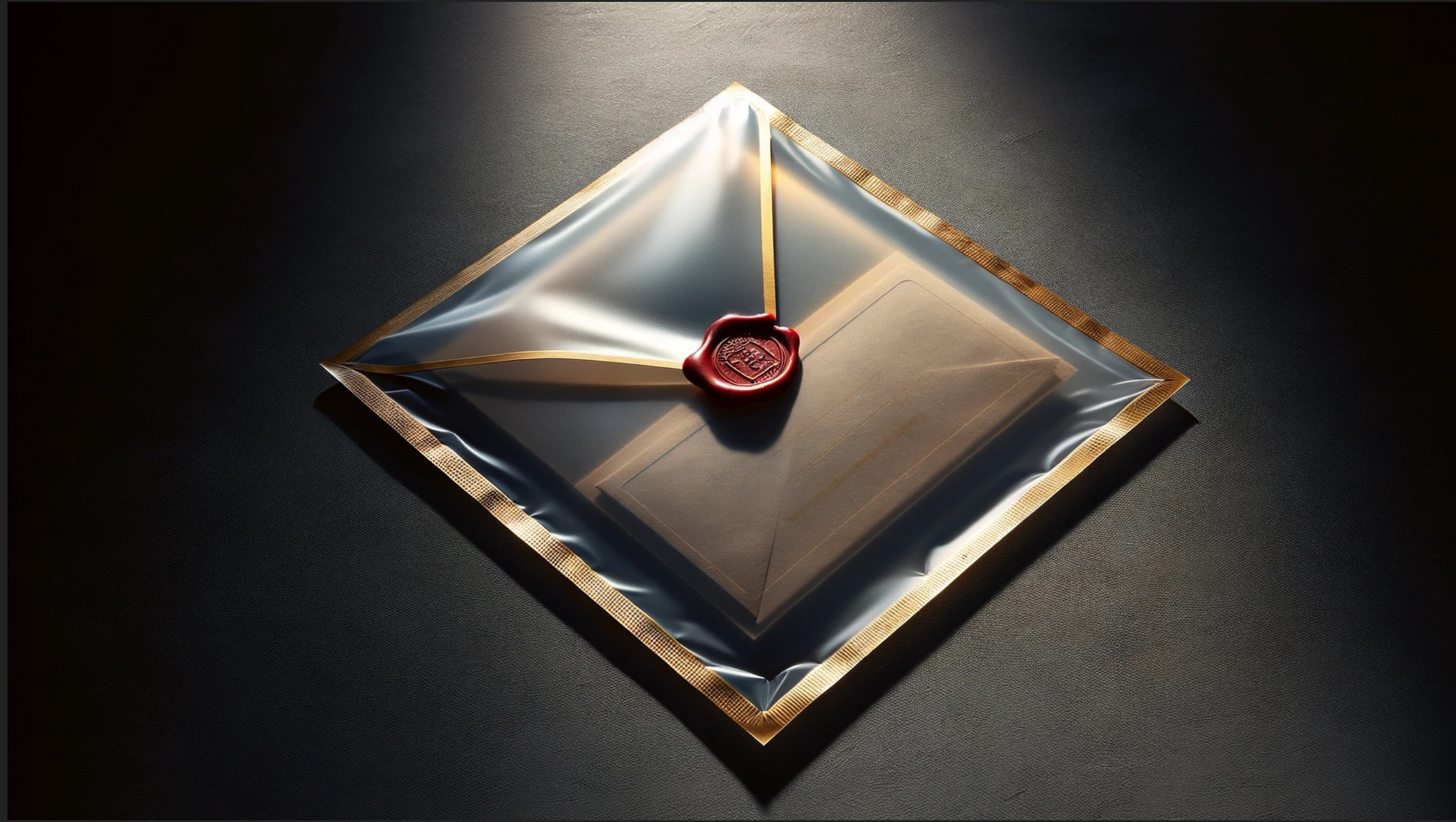
EXTENSIONS: GORDIAN SEALED TRANSACTION PROTOCOL (GSTP)



```
{
  request(ARID(c66be27d)) [
    'body': «do_it» [
      <arg1>: Type1
      <arg2>: Type2
    ]
    'senderPublicKey': PublicKeyBase
    'senderContinuation': ENCRYPTED [
      'hasRecipient': SealedMessage
    ]
    'recipientContinuation': ENCRYPTED [
      'hasRecipient': SealedMessage
    ]
  ]
} [
  'verifiedBy': Signature
]
```

Encrypted State
Continuations
(ESC)

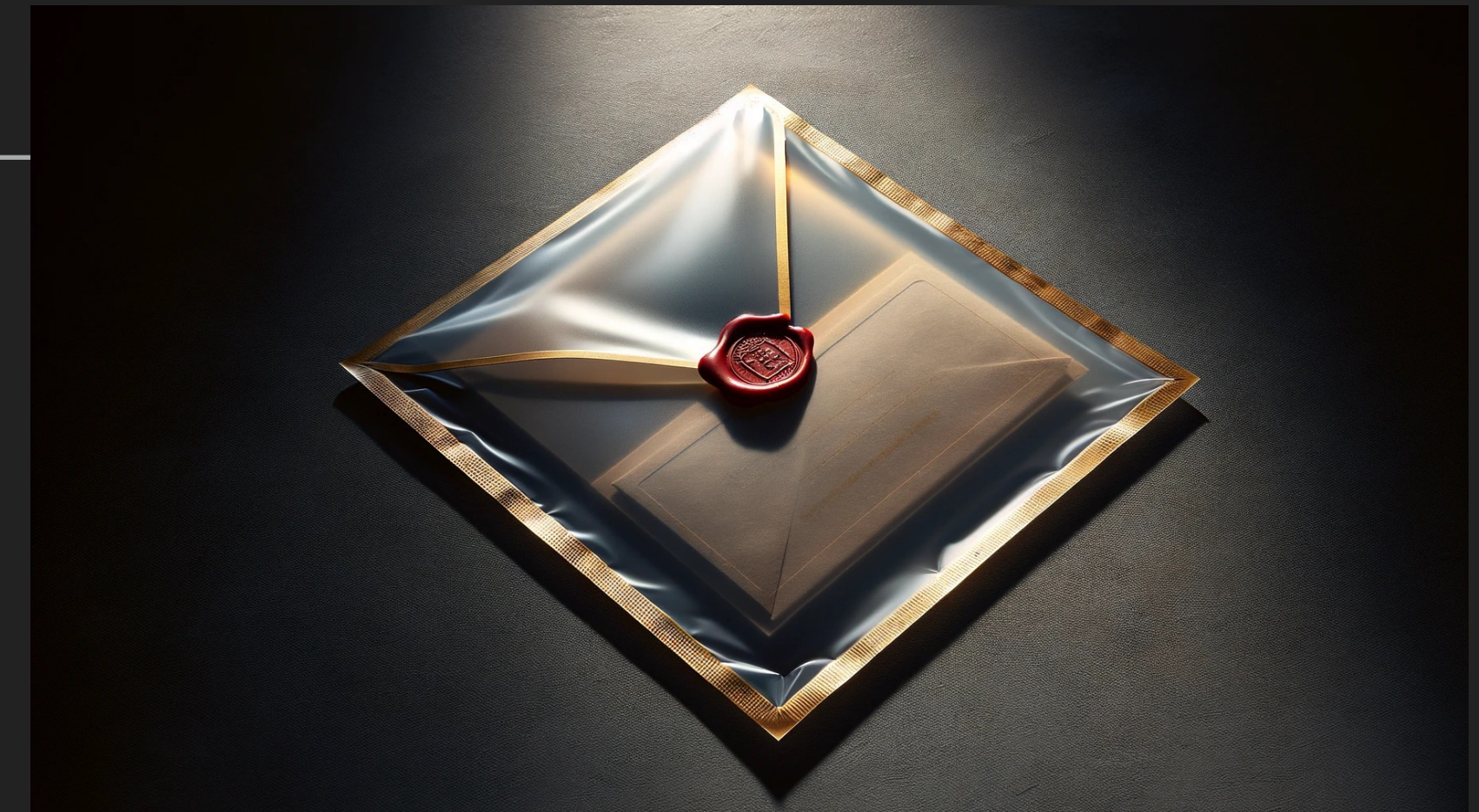




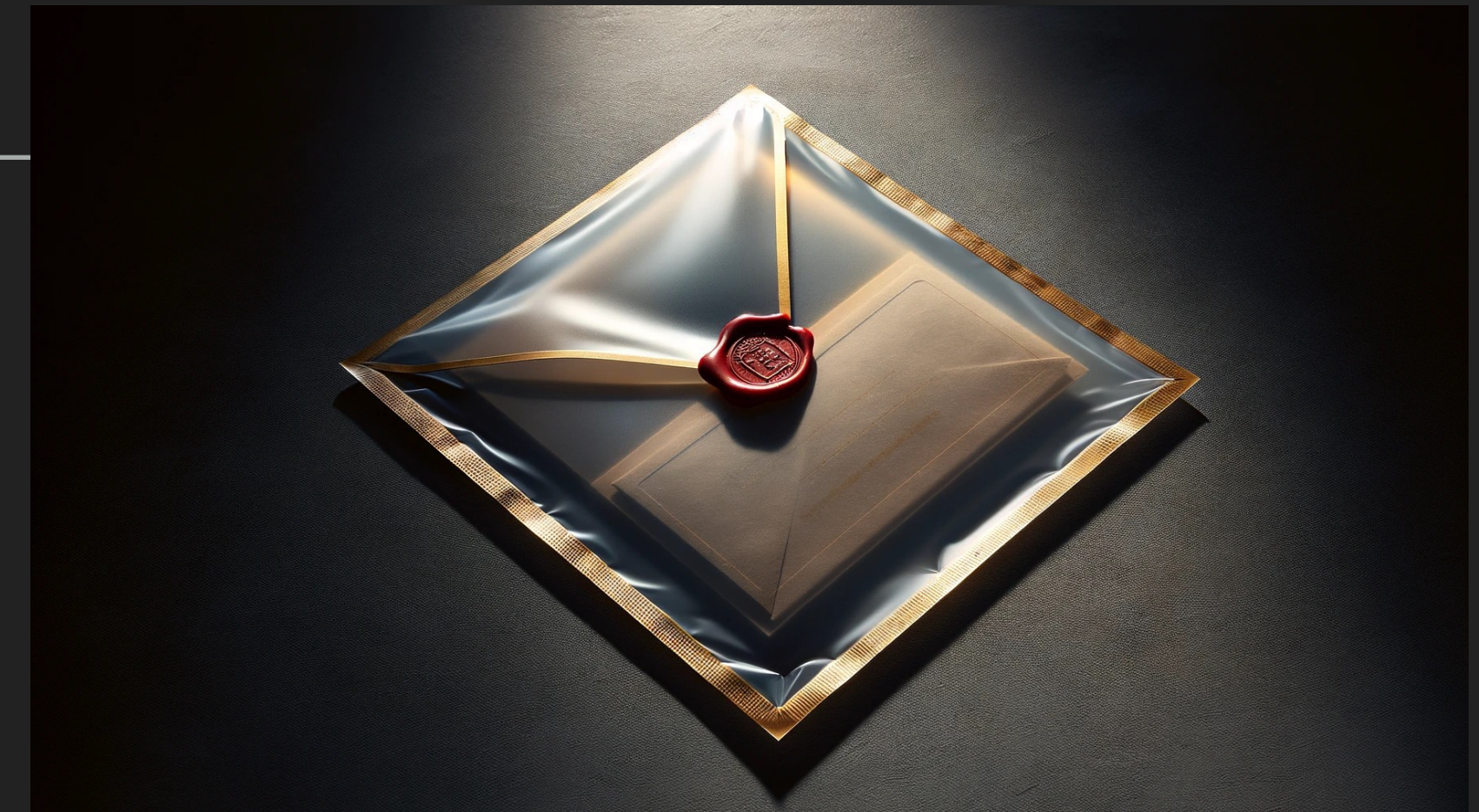
IMPROVING ON CONTROLLER DOCUMENTS

WAYS TO IMPROVE CONTROLLER DOCUMENTS

- ▶ CBOR-LD
- ▶ Bespoke CBOR
- ▶ Gordian Envelope 🙌
 - ▶ Why?
 - ▶ All the flexibility and advantages we've talked about
 - ▶ Holder-based elision 🎉
 - ▶ With DIDs, you have to reveal a method and verification key
 - ▶ But with an envelope you can elide additional keys or endpoints
 - ▶ And verifiably reveal them at a later time



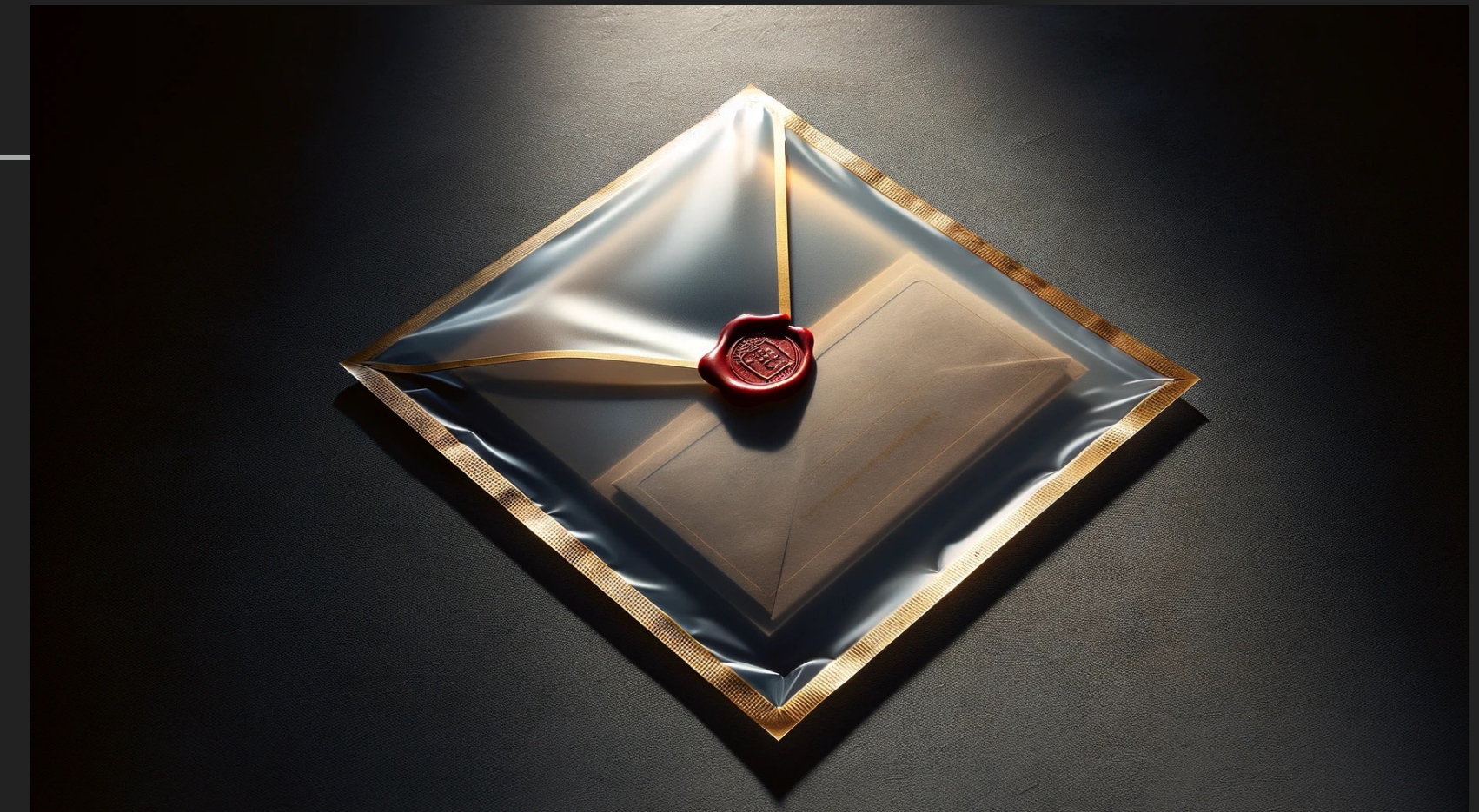
ELIDING A CONTROLLER DOCUMENT



```
{
  XID(2d9296d0) [
    'allow': 'all'
    'dereferenceVia': "https://resolver.example.com"
    'key': SigningPublicKey
    'key': 'group' [
      'controller': XID(5802b4ff) [
        'dereferenceVia': "btc:01234567"
      ]
      'key': SigningPublicKey [
        'deny': 'verify'
      ]
      'key': AgreementPublicKey [
        'endpoint': "https://messaging.example.com"
      ]
    ]
  ]
} [
  'verifiedBy': Signature
]
```



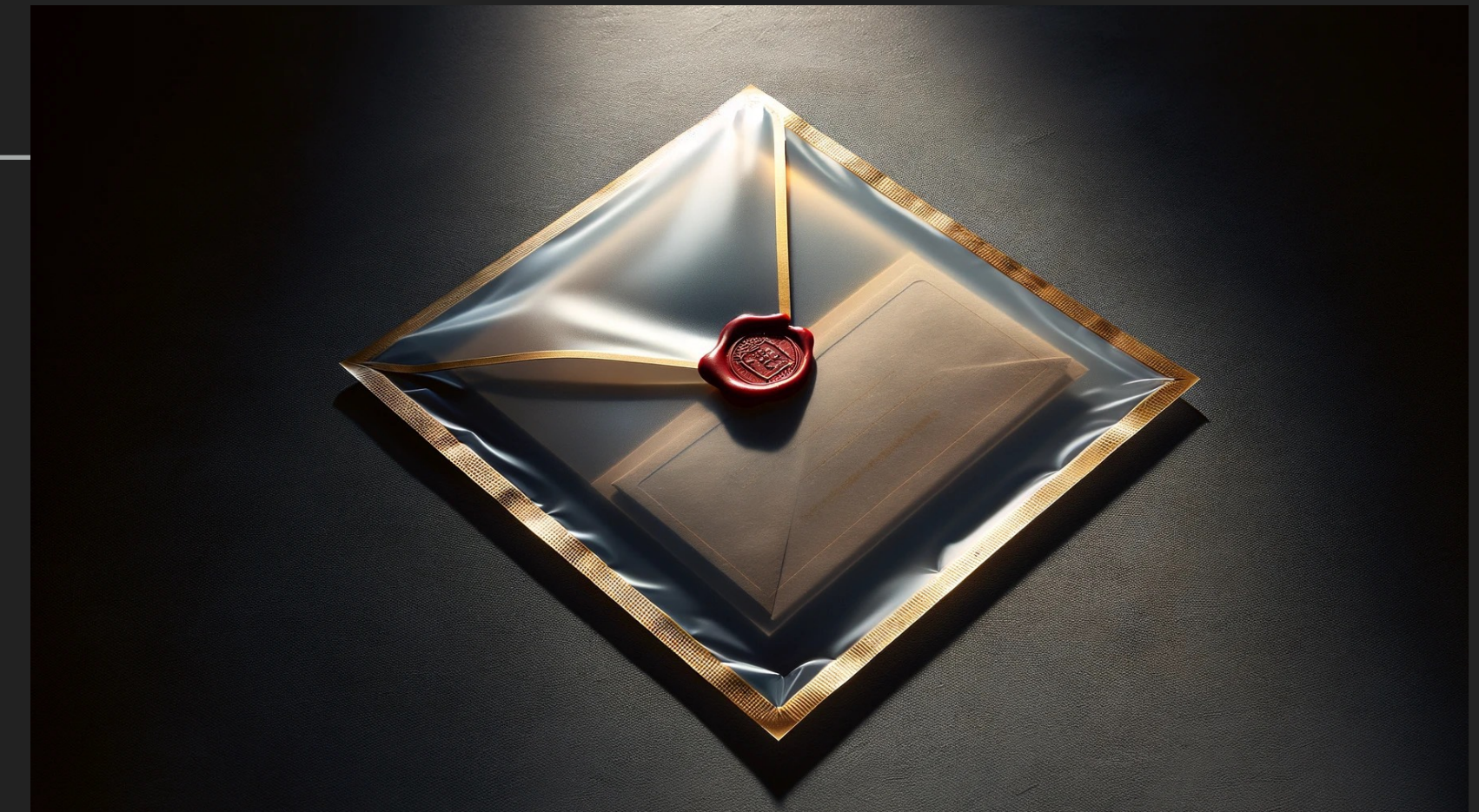
ELIDING A CONTROLLER DOCUMENT



```
{
  XID(2d9296d0) [
    'allow': 'all'
    'dereferenceVia': "https://resolver.example.com"
    'key': SigningPublicKey [
      'salt': Salt
    ]
    'key': 'group' [
      'controller': XID(5802b4ff) [
        'dereferenceVia': "btc:01234567"
        'salt': Salt
      ]
      'key': SigningPublicKey [
        'deny': 'verify'
        'salt': Salt
      ]
      'key': AgreementPublicKey [
        'endpoint': "https://messaging.example.com"
        'salt': Salt
      ]
    ]
  ]
} [
  'verifiedBy': Signature
]
```



ELIDING A CONTROLLER DOCUMENT

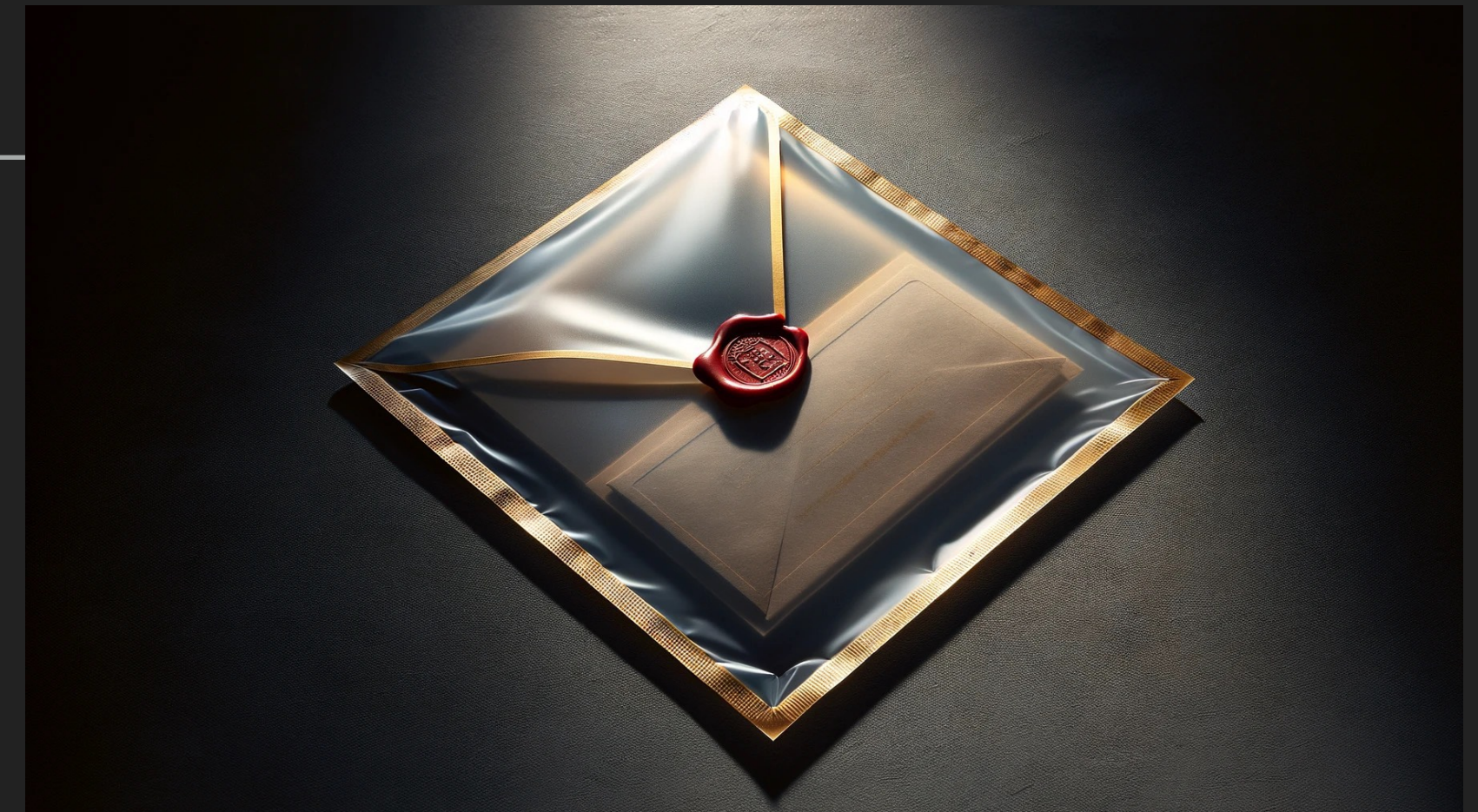


```
{
  XID(2d9296d0) [
    'allow': 'all'
    'key': SigningPublicKey [
      ELIDED
    ]
    'key': 'group' [
      'key': AgreementPublicKey [
        'endpoint': "https://messaging.example.com"
        ELIDED
      ]
      ELIDED (3)
    ]
    ELIDED
  ]
} [
  'verifiedBy': Signature
]
```



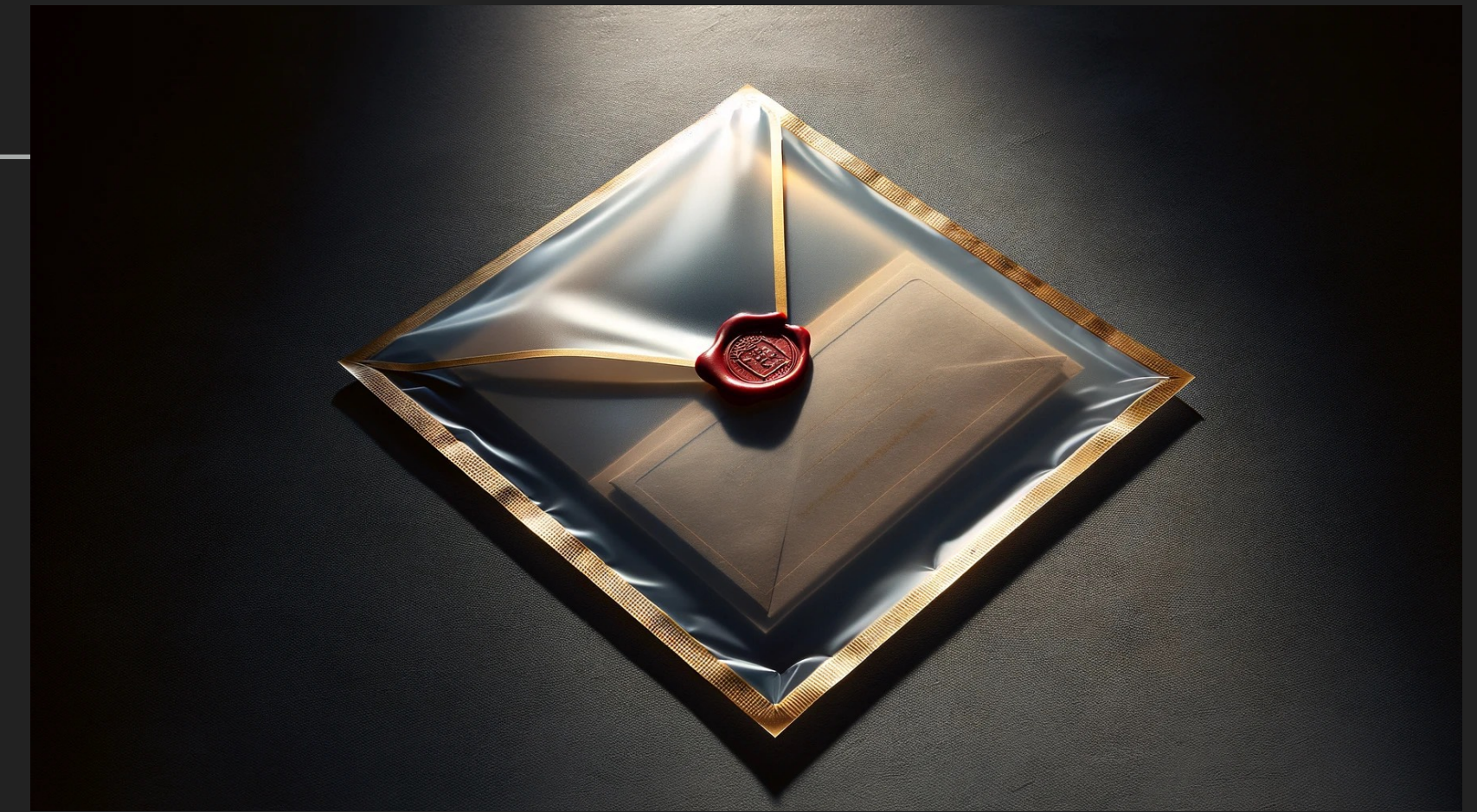
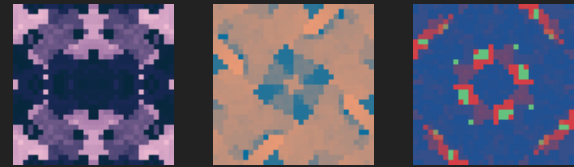
ELIDING A CONTROLLER DOCUMENT

```
{  
  XID(2d9296d0) [  
    'key': SigningPublicKey  
    ELIDED (3)  
  ]  
} [  
  'verifiedBy': Signature  
]
```



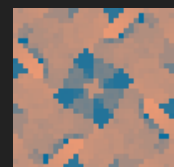
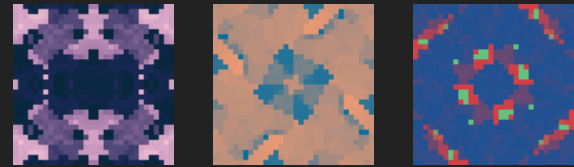
ELIDING A CONTROLLER DOCUMENT

```
{  
  XID(2d9296d0) [  
    'key': SigningPublicKey  
    ELIDED (3)  
  ]  
} [  
  'verifiedBy': Signature  
]
```

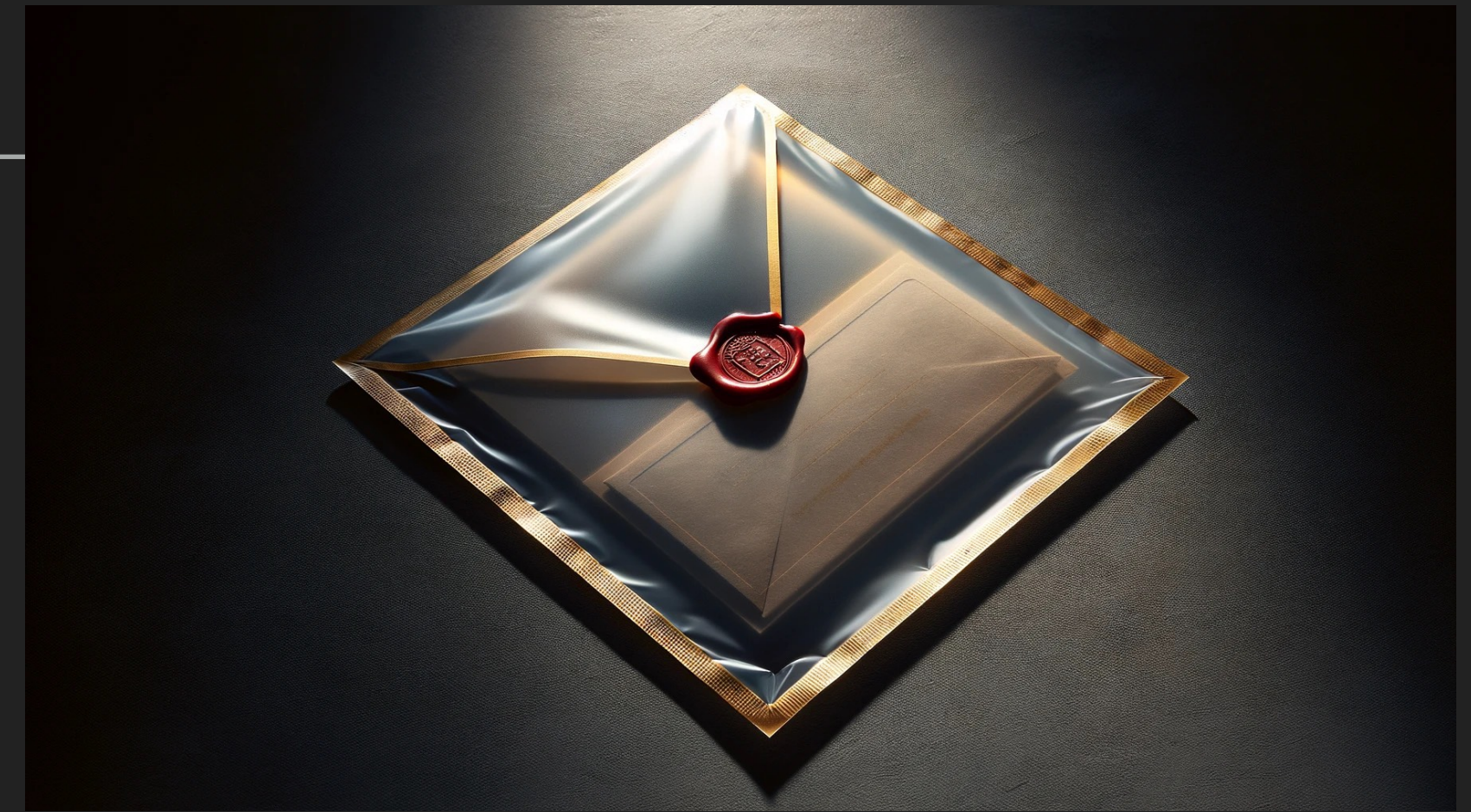


ELIDING A CONTROLLER DOCUMENT

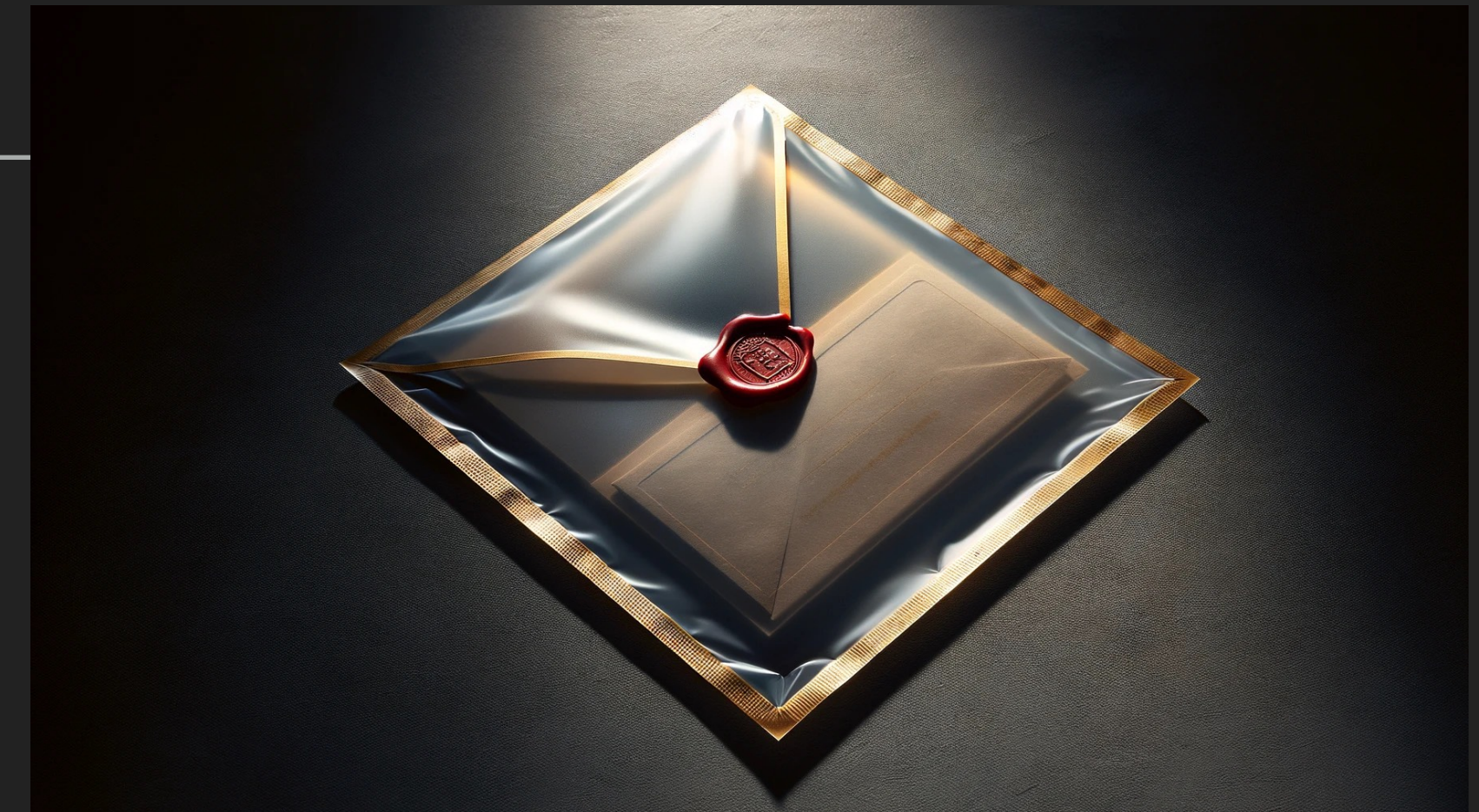
```
{  
  XID(2d9296d0) [  
    'key': SigningPublicKey  
    ELIDED (3)  
  ]  
} [  
  'verifiedBy': Signature  
]
```



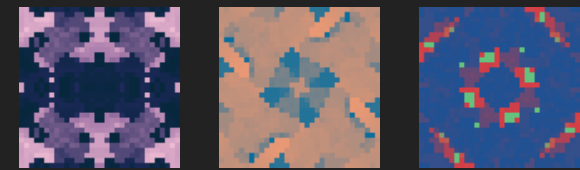
Inclusion Proof



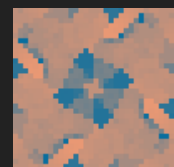
ELIDING A CONTROLLER DOCUMENT



```
{  
  XID(2d9296d0) [  
    'key': SigningPublicKey  
    ELIDED (3)  
  ]  
} [  
  'verifiedBy': Signature  
]
```



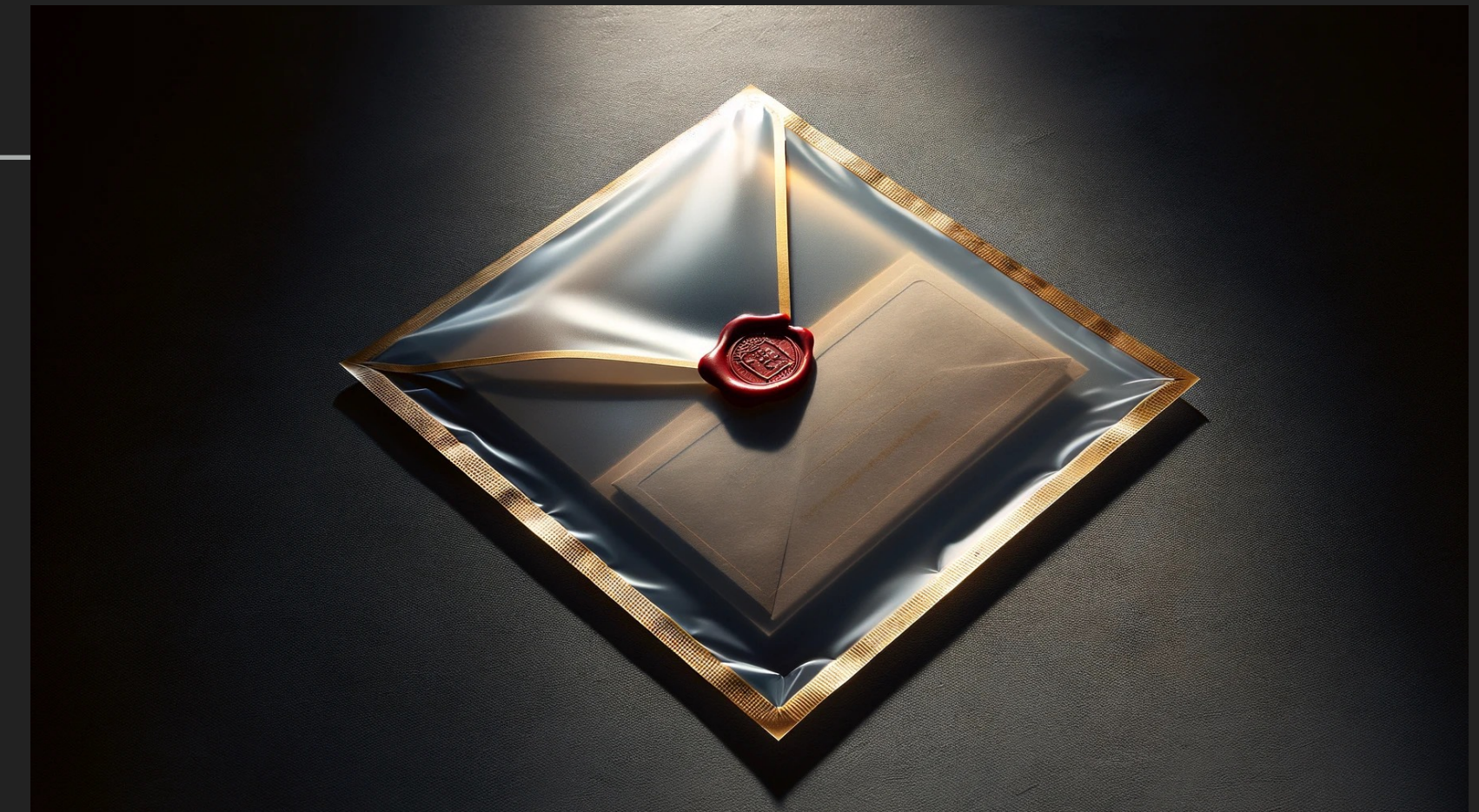
```
ELIDED [  
  'key': AgreementPublicKey [  
    ELIDED (2)  
  ]  
  ELIDED (3)  
]
```



Inclusion Proof

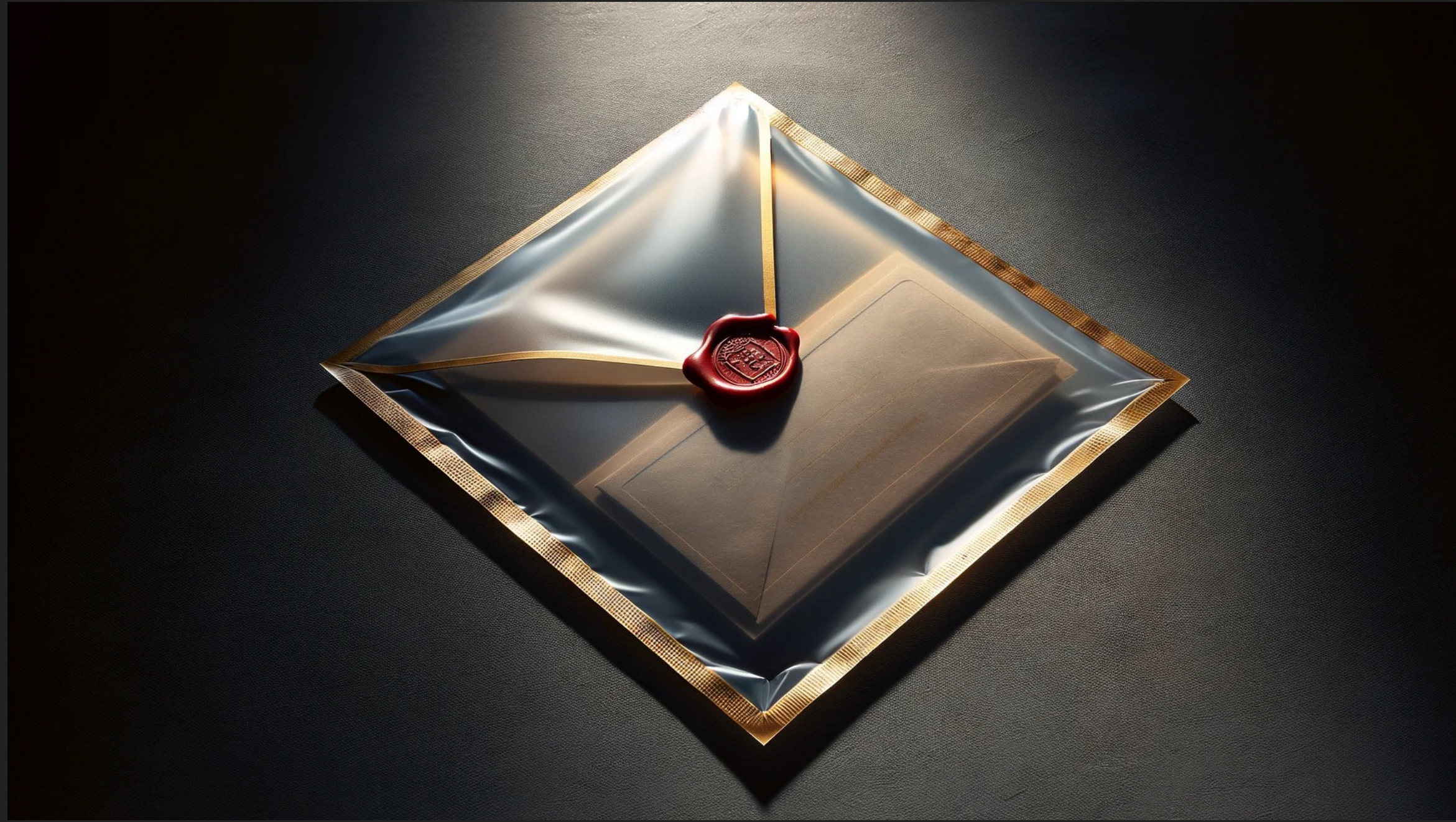


ELIDING A CONTROLLER DOCUMENT



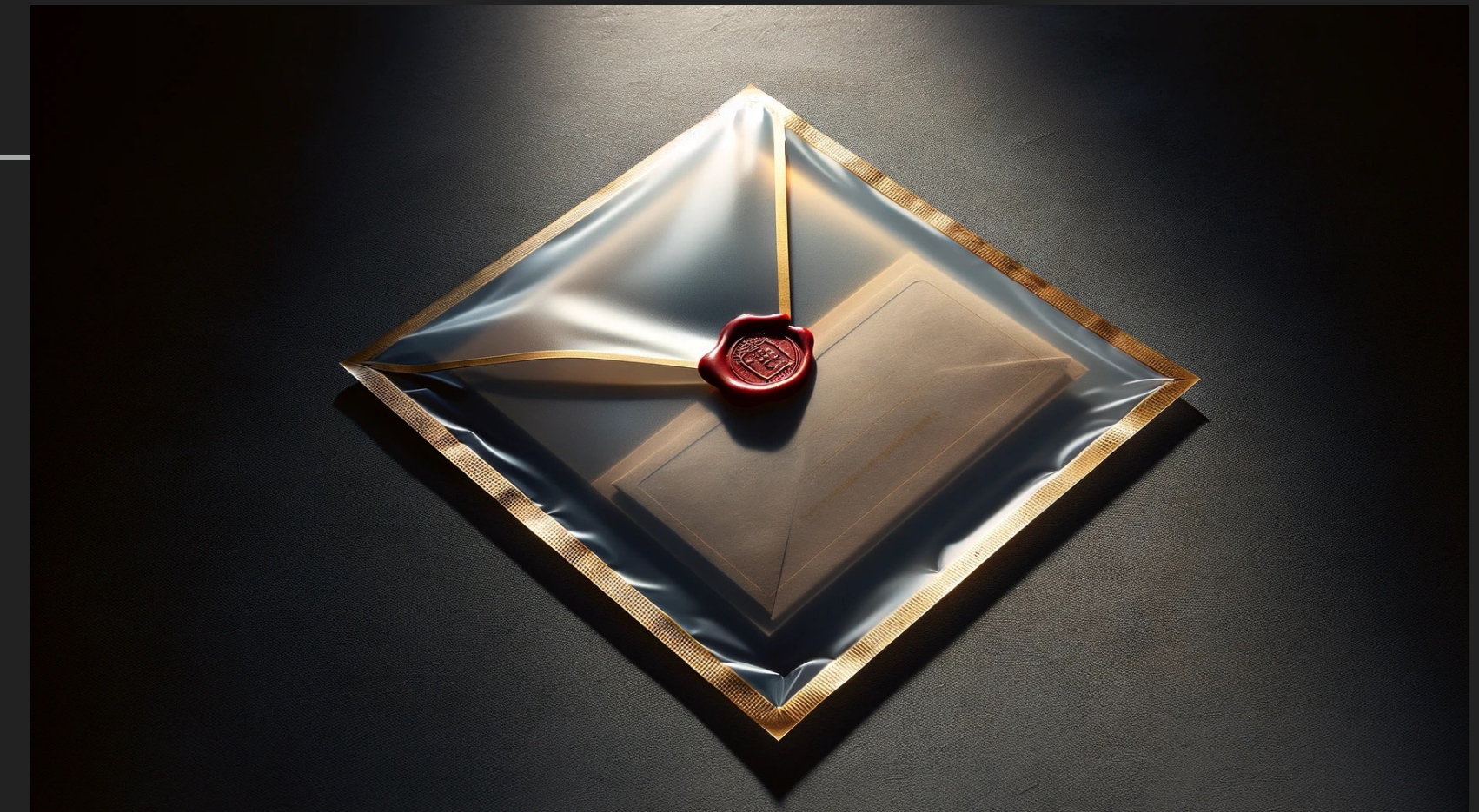
```
{  
  [XID(2d9296d0) [  
    'key': SigningPublicKey  
    ELIDED (2)  
    ELIDED [  
      'key': AgreementPublicKey [  
        ELIDED (2)  
      ]  
      ELIDED (3)  
    ]  
  ]  
} [  
  'verifiedBy': Signature  
]
```





**INTEGRATING WITH EXISTING
INFRASTRUCTURE**

INTEGRATING WITH EXISTING INFRASTRUCTURE

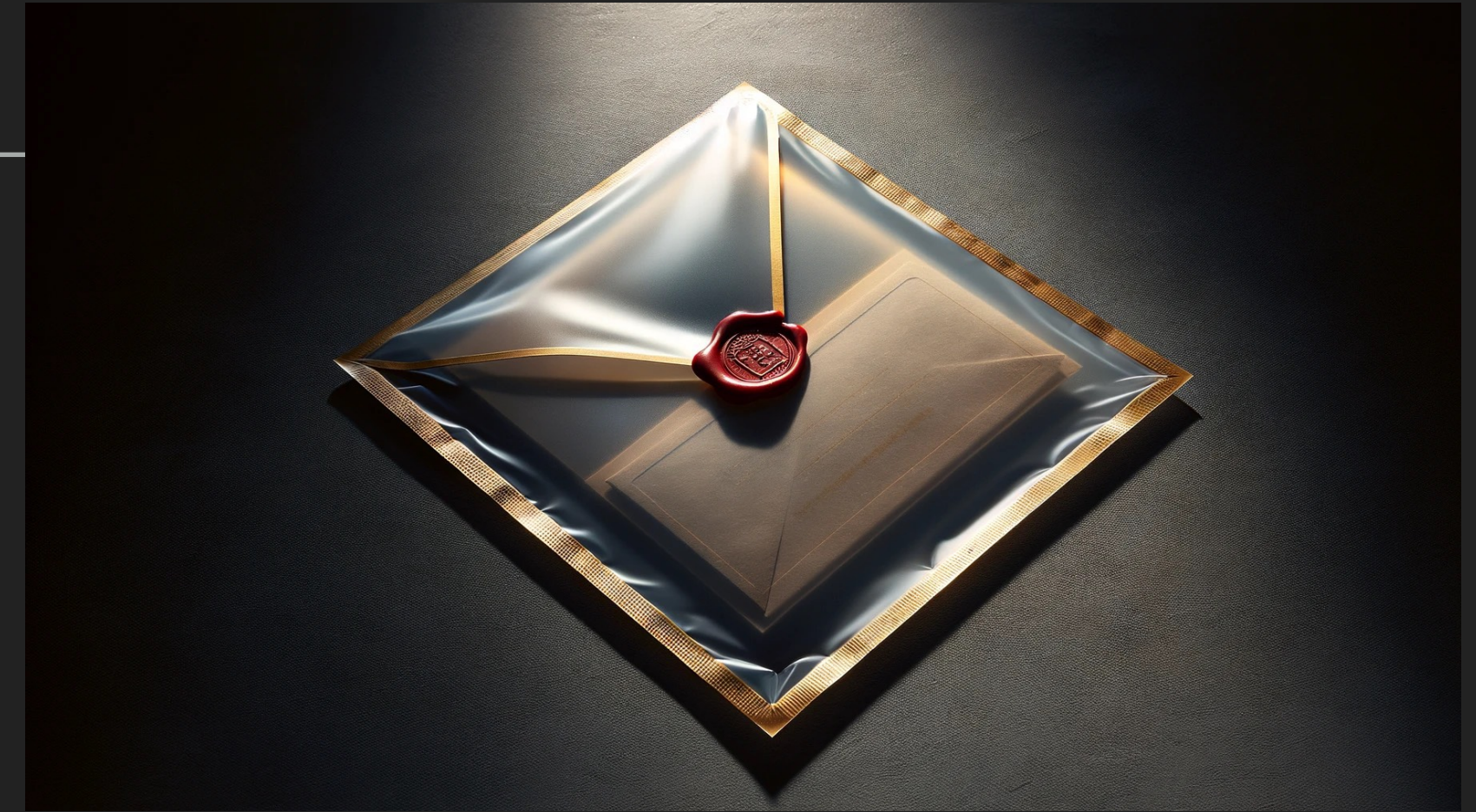


```
"did:example:123456789abcdefghi" [  
  'service': "https://example.com" [  
    'isA': 'LinkedDomainsEndpoint'  
    'salt': Salt  
  ]  
  'service': "https://messaging.example.com" [  
    'isA': 'MessagingEndpoint'  
    'salt': Salt  
  ]  
]
```

Envelope



INTEGRATING WITH EXISTING INFRASTRUCTURE

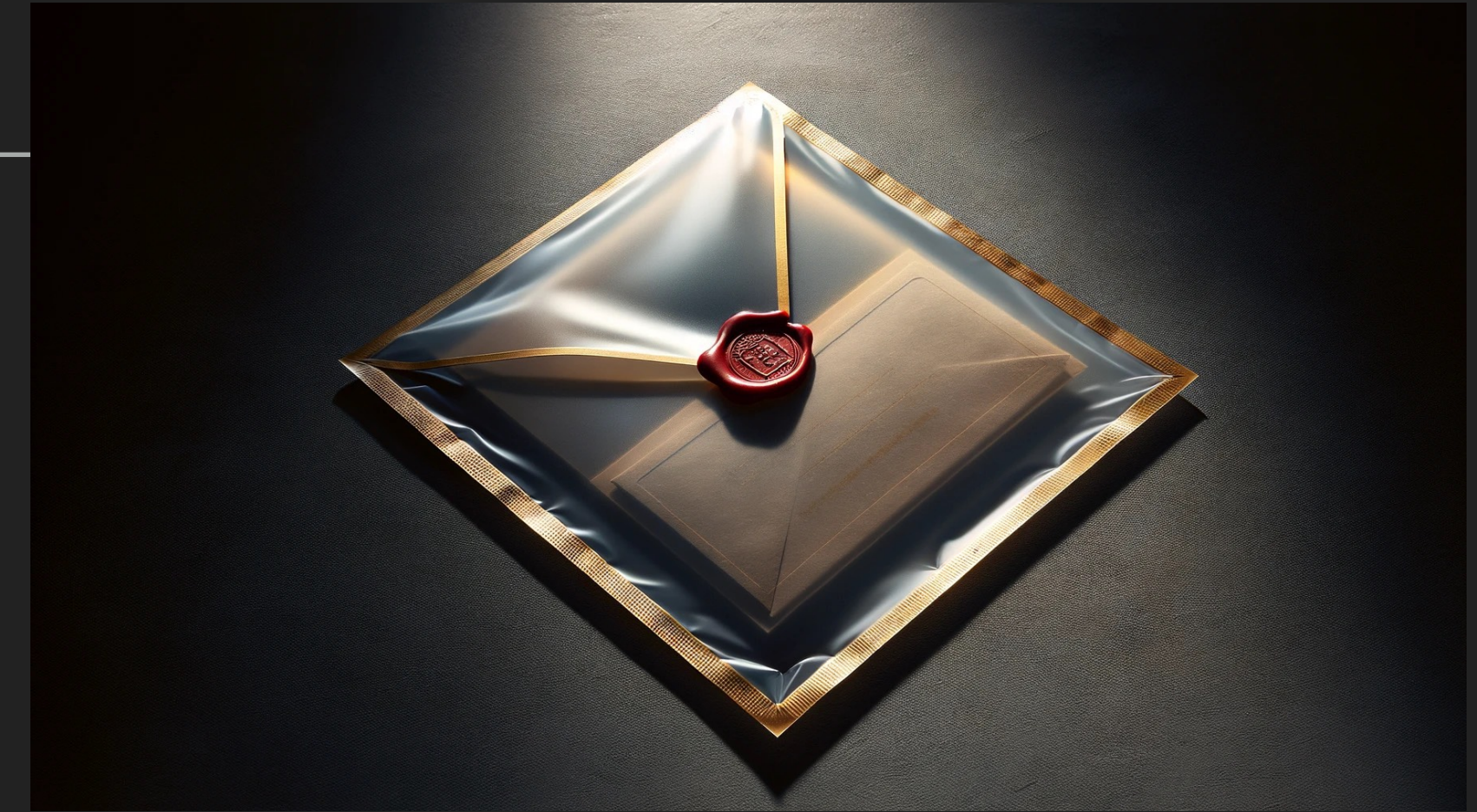


```
"did:example:123456789abcdefghi" [  
  ELIDED (2)  
]
```

Envelope



INTEGRATING WITH EXISTING INFRASTRUCTURE

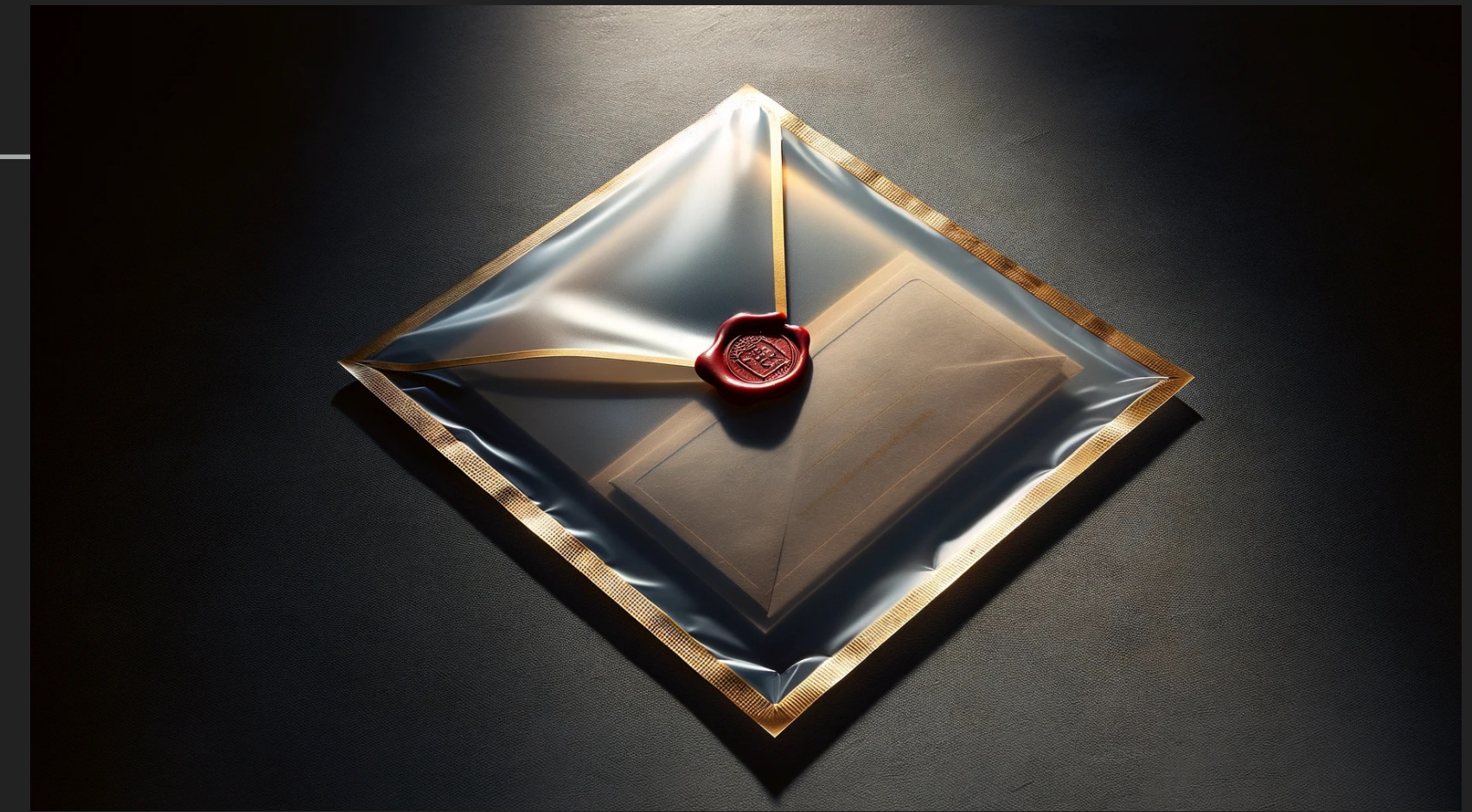


```
"cbor:<base-64 encoded envelope>"
```

JSON



INTEGRATING WITH EXISTING INFRASTRUCTURE



```
{  
  // ...  
  "service": [  
    {  
      "type": "ElidedServices",  
      "serviceEndpoint": "cbor:<base-64 encoded envelope>"  
    }  
  ]  
  // ...  
}
```

JSON



CHRISTOPHER ALLEN

christophera@lifewithalacrity.com



[@BlockchainComms](https://twitter.com/BlockchainComms)

WOLF MCNALLY

wolf@wolfmcnally.com



[@WolfMcNally](https://twitter.com/WolfMcNally)

